

messaging applications. Individuals engaged in criminal activity often store such records in order to, among other things, keep track of co-conspirator's contact information, keep a record of requests for payments or of payments made, and follow-up on requests for payments, contributions, or other aspects of the schemes. Based on my training and experience, I also know that once records are backed up to an iCloud, they can exist there for months or even years after they were created, even if a user replaces an iPhone or removes files from an iPhone device. Indeed, I have learned from publicly-available information from Apple that, depending on a user's settings, even if a user removes files from an iPhone, that user would need to log into their iCloud account and manually delete those same files in order for them to be removed from the iCloud account. Accordingly, there is reason to believe that records will be found in the Subject Accounts that date back years.

B. Evidence, Fruits and Instrumentalities

59. Based upon the foregoing, I respectfully submit there is probable cause to believe that the Subject Device, which contains the contents of the Subject Accounts, will contain evidence, fruits, and instrumentalities of the Subject Offenses, as more fully described in Section II of Attachment A to the proposed warrant. In particular, I believe the Subject Accounts are likely to contain the following information:

- a. Evidence related to any false statements or documents made or caused to be made to the Federal Election Commission.
- b. Evidence relating to the May 9, 2018 letter from Congressman [REDACTED] to Secretary of State [REDACTED] regarding U.S. Ambassador [REDACTED], including correspondence attaching or concerning the letter.

c. Communications with individuals associated with the government or a political party in the Ukraine, including [REDACTED].

d. Communications regarding [REDACTED] specifically or the position of U.S. Ambassador to Ukraine generally.

e. Evidence, including travel records, related to meetings with Ukrainian government officials involving Rudolph Giuliani, [REDACTED] Parnas, or Fruman.

f. Evidence of knowledge of the foreign agent registration laws and requirements, or lobbying laws, including but not limited to knowledge of the requirement to register as an agent of a foreign principal, or of the prohibition of acting on behalf of, lobbying for, or making contributions on behalf of a foreign principal.

g. Evidence of the intent of Parnas, Igor Fruman, [REDACTED], David Correia, Andrey Kukushkin, Andrey Muraviev, Giuliani, [REDACTED], [REDACTED] and [REDACTED], as it relates to the Subject Offenses under investigation.

III. Procedures for Searching ESI

A. Review of ESI

60. Law enforcement personnel (including, in addition to law enforcement officers and agents, and depending on the nature of the ESI and the status of the investigation and related proceedings, attorneys for the government, attorney support staff, agency personnel assisting the government in this investigation, interpreters, and outside vendors or technical experts under government control) will review the ESI contained on the Subject Device for information responsive to the warrant.

61. In conducting this review, law enforcement personnel may use various methods to locate evidence, fruits, and instrumentalities of the Subject Offenses, including but not limited to undertaking a cursory inspection of all emails contained on the Subject Device. This method is

analogous to cursorily inspecting all the files in a file cabinet in an office to determine which paper evidence is subject to seizure. Although law enforcement personnel may use other methods as well, particularly including keyword searches, I know that keyword searches and similar methods are typically inadequate to detect all information subject to seizure. As an initial matter, keyword searches work only for text data, yet many types of files commonly associated with emails, including attachments such as scanned documents, pictures, and videos, do not store data as searchable text. Moreover, even as to text data, keyword searches cannot be relied upon to capture all relevant communications in an account, as it is impossible to know in advance all of the unique words or phrases that investigative subjects will use in their communications, and consequently there are often many communications in an account that are relevant to an investigation but that do not contain any keywords that an agent is likely to search for.

IV. Conclusion and Ancillary Provisions

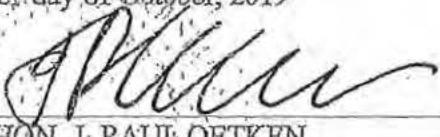
62. Based on the foregoing, I respectfully request the court to issue a warrant to seize the items and information specified in Attachment A to this affidavit and to the Search and Seizure Warrant.

63. The existence and scope of this ongoing criminal investigation is not publicly known. As a result, premature public disclosure of this affidavit or the requested warrant could alert potential criminal targets that they are under investigation, causing them to destroy evidence, flee from prosecution, or otherwise seriously jeopardize the investigation. Specifically, from my experience investigating public corruption and campaign finance offenses, I know that individuals who participate in such offenses communicate about known government investigations and sometimes tailor their stories to be consistent, and/or tamper with or hide potential evidence. In addition, the subjects of this investigation include dual citizens, who would have the ability and incentive to flee and evade prosecution. Accordingly, premature disclosure of the scope of this

investigation would undermine efforts to obtain truthful statements from relevant witnesses, and could lead to witness tampering, flight and/or obstruction of justice. Accordingly, there is reason to believe that, were the Providers to notify the subscriber or others of the existence of the warrant, the investigation would be seriously jeopardized. Pursuant to 18 U.S.C. § 2705(b), I therefore respectfully request that the Court direct the Providers not to notify any person of the existence of the warrant for a period of one year from issuance, subject to extension upon application to the Court, if necessary.

64. For similar reasons, I respectfully request that this affidavit and all papers submitted herewith be maintained under seal until the Court orders otherwise, except that the Government be permitted without further order of this Court to provide copies of the warrant and affidavit as need be to personnel assisting it in the investigation and prosecution of this matter, and to disclose those materials as necessary to comply with discovery and disclosure obligations in any prosecutions related to this matter.

Sworn to before me on
21 day of October, 2019


HON. J. PAUL OETKEN
UNITED STATES DISTRICT JUDGE

Attachment A**I. Device to be Searched**

The device to be searched (the “Subject Device”) is described as a hard drive containing the contents of the below four iCloud accounts, which were obtained pursuant to a search warrant authorized on or about May 16, 2019, by the Honorable Stewart Aaron, Magistrate Judge for the Southern District of New York, criminal number 19 Mag. 4784:

<i>iCloud Account</i>	<i>Owner</i>	<i>Referred To As</i>
[REDACTED]	Lev Parnas	Subject Account-1
[REDACTED]	Lev Parnas	Subject Account-2
[REDACTED]	Igor Fruman	Subject Account-3
[REDACTED]	[REDACTED]	Subject Account-4 (collectively, the “Subject Accounts”)

II. Review of ESI on the Subject Device

Law enforcement personnel (including, in addition to law enforcement officers and agents, and depending on the nature of the ESI and the status of the investigation and related proceedings, attorneys for the government, attorney support staff, agency personnel assisting the government in this investigation, interpreters, and outside vendors or technical experts under government control) are authorized to review the ESI contained on the Subject Accounts for evidence, fruits, and instrumentalities of one or more violations of 18 U.S.C. § 1519 (fabrication of documents); 22 U.S.C. §§ 612 and 618 (failure to register as a foreign agent); 18 U.S.C. § 951 (acting as an agent of a foreign government); and 18 U.S.C. § 1343 (wire fraud) (together, the “Subject Offenses”), as listed below:

- a. Evidence related to any false statements or documents made or caused to be made to the Federal Election Commission.
- b. Evidence relating to the May 9, 2018 letter from Congressman [REDACTED] to Secretary of State [REDACTED] regarding U.S. Ambassador [REDACTED], including correspondence attaching or concerning the letter.
- c. Communications with individuals associated with the government or a political party in the Ukraine, including [REDACTED], [REDACTED], or [REDACTED].
- d. Communications regarding [REDACTED] specifically or the position of U.S. Ambassador to Ukraine generally.
- e. Evidence, including travel records, related to meetings with Ukrainian government officials involving Rudolph Giuliani, [REDACTED] Parnas, or Fruman.
- f. Evidence of knowledge of the foreign agent registration laws and requirements, or lobbying laws, including but not limited to knowledge of the requirement to register as an agent of a foreign principal, or of the prohibition of acting on behalf of, lobbying for, or making contributions on behalf of a foreign principal.

g. Evidence of the intent of Parnas, Igor Fruman, [REDACTED], David Correia, Andrey Kukushkin, Andrey Muraviev, Giuliani, [REDACTED] and [REDACTED] as it relates to the Subject Offenses under investigation.